



Certified Ethical Hacker v7

Course Description

Prepare for the CEH certification while learning the latest ethical hacking techniques.

If you're concerned about the integrity of your network's infrastructure, you need the ethical hacking tools and techniques you will learn in Certified Ethical Hacker (CEH) v7 to enhance your network's defenses. You'll begin by learning how perimeter defenses work. Then, by scanning and attacking your own network (no real networks will be harmed), you'll learn how intruders operate and the steps you can take to secure a system.

In the interactive, lab-filled environment of this ethical hacking course, you will gain in-depth knowledge and practical experience with current, essential security systems. You will explore common ethical hacking topics, such as intrusion detection, policy creation, social engineering, DDoS attacks, buffer overflows, and virus creation. In addition to learning how to scan, test, hack, and secure a system, you'll prepare for the latest Certified Ethical Hacker exam from EC-Council.

Audience Profile

This course will significantly benefit security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure.

Course Objective

Candidates will learn:

- Footprinting and reconnaissance
- Hacking web servers, web applications, and wireless networks
- Cryptography
- Penetration testing
- Social engineering
- Trojans, viruses, and worms
- Evading IDS, firewalls, and honeypots
- Enumeration
- Buffer overflows

Duration

5 days

Pre-requisites

At least two years of IT security experience and a strong working knowledge of TCP/IP. Security+ Prep Course is highly recommended.

Course Outline

1. Introduction to Ethical Hacking
2. Footprinting and Reconnaissance
3. Scanning Networks
4. Enumeration
5. System Hacking
6. Trojans and Backdoors
7. Viruses and Worms
8. Sniffers
9. Social Engineering
10. Denial of Service
11. Session Hijacking
12. Hacking Web Servers
13. Hacking Web Applications
14. SQL Injection
15. Hacking Wireless Networks
16. Evading IDS, Firewalls, and Honeypots
17. Buffer Overflows
18. Cryptography
19. Penetration Testing